## Listing of the Claims

1.      (Currently amended)  A method ~~for implementing secure communication,~~ comprising:

(a)  ~~receiving instructions to initiate a process for creating a secure communication link to a remote device~~ initiating a connection via a publicly accessible network from a wireless device, wherein

the wireless device includes an unprovisioned virtual private network (VPN) program and an unprovisioned automatic content updating (ACU) program, and

the ACU program is configured, upon provisioning, to communicate with one or more remotely-located devices on behalf of at least one additional program that is distinct from the ACU and VPN programs;

~~(b)  determining, in response to the instructions received in step (a), whether at least one local application program used to create the secure communication link is configured;~~

~~(c)  initiating, based on the instructions received in step (a), a second process for accessing a database over the publicly accessible network;~~

~~(d)~~(b)  receiving, in the wireless device and using the connection. ~~response to step (c) and if the at-least one local application program is not configured. configuration~~ information for provisioning the ~~at least one~~ ACU program;

~~(e)~~(c)  ~~configuring~~ provisioning the ~~at least one~~ ACU program based upon the ~~configuration~~ information received in step ~~(d)~~(b); ~~and~~

(d)  receiving in the wireless device, via the publicly accessible network and using the provisioned ACU program, information for provisioning the VPN program;

(e)  provisioning the VPN program based upon the information received in step (d); and

(f)  creating ~~the~~ a secure communication link ~~based on~~ using the ~~configur~~ provisioned ~~ation~~ VPN program.


2.      (Currently amended)  The method of claim 1, wherein~~:~~

~~the secure communication link is a VPN connection, and~~

—————————the information received in step ~~(d)~~(b) comprises ~~at least one of a public/private key pair and a~~an ACU certificate corresponding to the wireless device and the information received in step (d) comprises a VPN certificate corresponding to the wireless device.

3.    (Currently amended)  The method of claim 1, further comprising:

(g)   determining whether an update to the ~~at least one~~VPN ~~application~~ program is available;

(h)   receiving the update; and

(i)   implementing the update.

4.    (Canceled)

5.    (Currently amended)  The method of claim 1, ~~wherein step (d) comprises receiving a generic VPN policy without PKI data, and~~ further comprising:

~~(g)  generating PKI data and a corresponding certificate enrollment request;~~

~~(h)~~(g)   sending, prior to step (d), a ~~the~~certificate enrollment request ~~to the remote device~~ for forwarding to an external certification authority (CA).~~; and~~

~~(i)  receiving a certificate.~~

6.    (Canceled)

7.    (Canceled)

8.    (Currently amended)  The method of claim ~~7~~1, ~~wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and~~ further comprising:

(g)   determining whether an update is available for the at least one ~~of the~~ additional ~~application programs;~~program; and

3

(h) receiving an update for the at least one additional ~~application~~ program.

9.    (Canceled)

10.    (Currently amended)   The method of claim ~~7~~1, ~~wherein the ACU application contains~~ ~~information about application programs in addition to the at least one local application program~~ ~~used to create the secure communication link, and~~ further comprising:

(g)  fetching, from <u>one of</u> the <u>one or more</u> remotely-<u>located</u> devices, content or content metadata applicable to <u>the</u> at least one ~~of the~~ additional ~~application programs;~~program; and

(h)  storing, by the at least one additional ~~application~~ program, the fetched content or content metadata.

11.    (Currently amended)   The method of claim ~~7~~1, wherein the ACU ~~application~~ program communicates using a SyncML protocol.

12.    (Currently amended)   The method of claim ~~7~~1, further comprising:

(g)  storing, in a configuration record for ~~at least one~~ the VPN ~~application~~program, an Internet Access Point (IAP) to be used when communicating with <u>one of</u> the <u>one or more</u>~~a~~ remotely-<u>located</u> devices on behalf of the ~~at least one~~VPN ~~application~~program.

13.    (Currently amended)   The method of claim ~~7~~1, wherein the ACU ~~application~~ program communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair.

14.    (Currently amended)   The method of claim ~~7~~1, ~~wherein the ACU application contains~~ ~~information about application programs in addition to the at least one local application program~~ ~~used to create the secure communication link, and~~ further comprising:

4

(g) fetching, from <u>one of</u> the <u>one or more</u> remote<u>ly-located</u> devices, content metadata applicable to <u>the</u> at least one ~~of the~~ additional ~~application programs;~~<u>program:</u>

(h) comparing fetched metadata to locally stored metadata; and

(i) fetching new or updated content from the <u>one of the one or more</u> remote<u>ly-located</u> device<u>s</u> based upon the comparison.

15.    (Currently amended)  The method of claim 14, wherein the ACU ~~application~~<u>program</u> includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the <u>one of the one or more remotely-located devices</u>~~remote device~~.

16.    (Currently amended)  The method of claim ~~7~~<u>1</u>, ~~wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and~~ further comprising:

(g) fetching, from multiple databases in <u>one of the one or more</u> ~~the~~ remote<u>ly-located</u> device<u>s</u>, metadata about multiple types of content.

17.    (Currently amended)  The method of claim ~~7~~<u>1</u>, wherein

———————— ~~the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and~~

————————the ACU ~~application~~<u>program</u> transmits requests containing properties used by <u>one of</u> the <u>one or more</u> remote<u>ly-located</u> device<u>s</u> to filter requests.

18.    (Currently amended)  The method of claim ~~7~~<u>1</u>, wherein messages generated by the ACU ~~application~~<u>program</u> and communicated to <u>one of</u> the <u>one or more</u> remote<u>ly-located</u> device<u>s</u> include a message identifier, a target database identifier, and a security level.

19.    (Currently amended)  The method of claim 18, wherein a first security level is required to receive configuration information for the ~~at least one~~VPN program and a second security level is required to receive another type of information.

20.    (Currently amended)  The method of claim 18, wherein at least one message generated by the ACU ~~application~~ program includes an element indicating that ~~a~~ the at least one message is ~~the~~ a last message relating to a specific task.

21.    (Currently amended)  The method of claim 18, wherein the ACU ~~application~~ program requests configuration information in a single message.

22.    (Currently amended)  The method of claim ~~7~~1 further comprising, ~~upon receipt of a first response from the remote device~~prior to step (b):

(g)  validating and storing a returned certificate corresponding to one of the one or more remotely-located devices so as to create a trust relationship with ~~the~~that remotely-located device.

23.    (Currently amended)  The method of claim 22, further comprising:

(h)  using the ~~returned~~ certificate stored in step (g) to validate subsequent responses from ~~the~~that remotely-located device.

24.    (Currently amended)  The method of claim 23, wherein:

the ~~returned~~ certificate corresponding to the one of the one or more remotely-located devices is validated based on a hash calculated over ~~the~~an entire ACU message ~~resulting in the first response from the remote device~~, except for a signature element of ~~the~~that ACU message,

the hash is signed with a private key held by the one of the one or more remotely-located devices~~remote device~~, and

6

the ~~corresponding~~ certificate corresponding to the one of the one or more remotely-located devices is included in ~~the~~ a first response from the one of the one or more remotely-located devices and is used by the ~~recipient~~ wireless device to verify the signature and identify and authenticate ~~the~~ a sender.

25. (Currently amended) An apparatus ~~device for secure communication with a server via a publicly accessible network,~~ comprising:

a transceiver configured to provide a wireless~~an~~ interface to a publicly accessible network; and

a processor configured to perform steps ~~comprising:~~ that include

(a) ~~receiving instructions to initiate a process for creating a secure communication link to a remote device~~ initiating a connection via ~~a~~ the publicly accessible ~~network;~~ network, wherein

the apparatus includes an unprovisioned virtual private network (VPN) program and an unprovisioned automatic content updating (ACU) program, and

the ACU program is configured, upon provisioning, to communicate with one or more remotely-located devices on behalf of at least one additional program that is distinct from the ACU and VPN programs.

~~(b) determining, in response to the instructions received in step (a), whether at least one local application program used to create the secure communication link is configured;~~

~~(c) initiating, based on the instructions received in step (a), a second process for accessing a database over the publicly accessible network;~~

~~(d)~~(b) receiving, ~~in response to step (c) and if the at least one local application program is not configured~~ using the connection,~~configuration~~ information for provisioning the ~~at least one~~ACU program,~~program;~~

~~(e)~~(c) ~~configuring the at least one~~ provisioning the ACU program based upon the ~~configuration~~ information received in step ~~(d);~~(b),~~and~~

(d) receiving, via the publicly accessible network and using the provisioned ACU program, information for provisioning the VPN program,

7

_____ (e)  provisioning the VPN program based upon the information received in step (d), and

(f)  creating ~~the~~ a secure communication link ~~based on the configuration~~ using the provisioned VPN program.

26.  (Currently amended)  The apparatus ~~device~~ of claim 25, wherein ~~:~~

~~the secure communication link is a VPN connection, and~~

~~the information received in step ~~(d)~~ (b) comprises ~~at least one of a public/private key pair and a~~ an ACU certificate corresponding to the apparatus and information received in step (d) comprises a VPN certificate corresponding to the apparatus.

27.  (Currently amended)  The apparatus ~~device~~ of claim 25, wherein the processor is further configured to perform steps ~~comprising:~~ that include

(g)  determining whether an update to the ~~at least one~~ VPN ~~application~~ program is ~~available:~~ available,

(h)  receiving the ~~update:~~ update, and

(i)  implementing the update.

28.  (Canceled)

29.  (Currently amended)  The apparatus ~~device~~ of claim ~~1~~ 25, ~~wherein step (d) comprises receiving a generic VPN policy without PKI data, and~~ wherein the processor is further configured to perform steps ~~comprising:~~ that include

~~(g)  generating PKI data and a corresponding certificate enrollment request;~~

~~(h)~~ (g)  sending, prior to step (d), a ~~the~~ certificate enrollment request ~~to the remote device~~ for forwarding to an external certification authority (CA).~~; and~~

~~(i)  receiving a certificate.~~

30.  (Canceled)

8

31.    (Canceled)

32.    (Currently amended)  The ~~apparatus~~ <u>device</u> of claim ~~31~~<u>25</u>, ~~wherein the ACU application~~ ~~contains information about application programs in addition to the at least one local application~~ ~~program used to create the secure communication link, and~~ wherein the processor is further configured to perform steps ~~comprising:~~<u>that include</u>

(g)  determining whether an update is available for <u>the</u> at least one ~~of the~~ additional ~~application programs:~~<u>program,</u> and

(h)  receiving an update for the at least one additional ~~application~~ program.

33.    (Canceled)

34.    (Currently amended)  The ~~apparatus~~ <u>device</u> of claim ~~31~~<u>25</u>, ~~wherein the ACU application~~ ~~contains information about application programs in addition to the at least one local application~~ ~~program used to create the secure communication link, and~~ wherein the processor is further configured to perform steps ~~comprising:~~<u>that include</u>

(g)  fetching, from <u>one of</u> the <u>one or more</u> remote<u>ly-located</u> device<u>s,</u> content or content metadata applicable to <u>the</u> at least one ~~of the~~ additional ~~application programs:~~<u>program,</u> and

(h)  storing, by the at least one additional ~~application~~ program, the fetched content or content metadata.

35.    (Currently amended)   The ~~apparatus~~ <u>device</u> of claim ~~31~~<u>25</u>, wherein the ACU ~~application~~<u>program</u> communicates using a SyncML protocol.

36.    (Currently amended)  The ~~apparatus~~ <u>device</u> of claim ~~31~~<u>25</u>, wherein the processor is further configured to perform steps ~~comprising:~~<u>that include</u>                .

9

(g)    storing, in a configuration record for ~~at least one~~the VPN ~~application~~program, an Internet Access Point (IAP) to be used when communicating with one of the one or more~~a~~ remotely-located device§ on behalf of the ~~at least one~~VPN ~~application~~program.

37.    (Currently amended)  The apparatus ~~device~~of claim ~~31~~25, wherein the ACU ~~application~~ program communicates using a simple request-response protocol, and wherein a protocol transaction consists of a single request-response pair.

38.    (Currently amended)  The apparatus ~~device~~of claim ~~31~~25, ~~wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and~~wherein the processor is further configured to perform steps ~~comprising:~~that include

(g)    fetching, from one of the one or more remotely-located device§, content metadata applicable to the at least one ~~of the~~additional ~~application programs:~~program,

(h)    comparing fetched metadata to locally stored ~~metadata:~~metadata, and

(i)    fetching new or updated content from the one of the one or more remotely-located device§ based upon the comparison.

39.    (Currently amended)  The apparatus ~~device~~of claim 38, wherein the ACU ~~application~~ program includes in fetch requests in steps (g) and (i) content identifications (IDs) required by the one of the one or more remotely-located devices~~remote device~~.

40.    (Currently amended)  The apparatus ~~device~~of claim ~~7~~25, ~~wherein the ACU application contains information about application programs in addition to the at least one local application program used to create the secure communication link, and~~wherein the processor is further configured to perform steps ~~comprising:~~that include

(g)    fetching, from multiple databases in one of the one or more~~the~~ remotely-located device§, metadata about multiple types of content.

10

41.     (Currently amended)  The ~~apparatus~~ device of claim ~~31~~25, wherein

——————————the ACU application contains information about application programs in addition
to the at least one local application program used to create the secure communication link, and

——————————the ACU ~~application~~ program transmits requests containing properties used by
one of the one or more remotely-located devices to filter requests.


42.     (Currently amended)  The ~~apparatus~~ device of claim ~~31~~25, wherein messages generated
by the ACU ~~application~~ program and communicated one of the one or more to the remotely-
located devices include a message identifier, a target database identifier, and a security level.


43.     (Currently amended)  The ~~apparatus~~ device of claim 42, wherein a first security level is
required to receive configuration information for the ~~at least one~~ VPN program and a second
security level is required to receive another type of information.


44.     (Currently amended)  The ~~apparatus~~ device of claim 42, wherein at least one message
generated by the ACU ~~application~~ program includes an element indicating that ~~a~~ the at least one
message is ~~the~~ a last message relating to a specific task.


45.     (Currently amended)  The ~~apparatus~~ device of claim 42, wherein the ACU ~~application~~
program requests configuration information in a single message.


46.     (Currently amended)  The ~~apparatus~~ device of claim ~~31~~25, wherein the processor is
further configured to perform steps ~~comprising~~ that include, ~~upon receipt of a first response from
the remote device~~:

        (g) validating and storing a returned certificate corresponding to one of the one or more
remotely-located devices so as to create a trust relationship with ~~the~~ that remotely-located device.


11

47.    (Currently amended)  The apparatus ~~device~~ of claim 46, wherein the processor is further configured to perform steps ~~comprising:~~that include

(h)  using the ~~returned~~ certificate stored in step (g) to validate subsequent responses from ~~the~~ that remotely-located device.

48.    (Withdrawn)  A server, comprising:

an interface to a publicly accessible network; and

a processor configured to perform steps comprising:

(a)  receiving requests from multiple users for configuration information for locally stored application programs used to create secure communication links to the server, the users being organized in a hierarchy of child, parent and grandparent groups, each group having a corresponding set of secure communication configuration data accessible by the server, each child group inheriting properties from its parent group, each parent group inheriting properties its grandparent group;

(b)  storing content associated with the groups, with information associated with a particular group being accessible to the particular group and to groups inheriting properties from the particular group;

(b)  providing configuration information to the users, the configuration information provided to each user comprising the configuration data set for each group from which the user inherits properties;

(c)  receiving requests from the users for content corresponding to other locally stored application programs; and

(d)  providing information to the users of a child group based on the groups from which the child group inherits properties.

49.    (New)  The method of claim 22, wherein step (g) includes requiring input of multiple characters from a user of the wireless device.

50.     (New)   The method of claim 49, wherein the multiple characters are a portion of an identifier for the certificate corresponding to one of the one or more remotely-located devices.

51.     (New)   The apparatus of claim 46, wherein step (g) includes requiring input of multiple characters from a user of the apparatus.

52.     (New)   The apparatus of claim 51, wherein the multiple characters are a portion of an identifier for the certificate corresponding to one of the one or more remotely-located devices.